

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/23/2012

To: Washington Field  
New York

Attn: CY-4

CY-2, SA [redacted]

From: Washington Field

CY4/NVRA

Contact: [redacted]

*o/a Full Investigation Assign to SA* [redacted]

b6  
b7C

Approved By: [redacted]

*ke 04/25/12*

A (Main/Sub [redacted])

Closed: C4 / C5 / C6

Class & Alpha *2028-WF--*

Source *DB*

Drafted By: [redacted]

*lj*

CPI/Codes (1) *CRINT-C*

*4/25/2012*  
*BA*  
*2028-WF--*

Case ID #: [redacted]

(Pending)

PI [redacted] Full [redacted]

Begins [redacted] Expires [redacted]

Assign To [redacted]

b7E

Title: UGNAZI;

TEAM-DIVERSITY;

DC.GOV - VICTIM;

COMPUTER INTRUSION - CRIMINAL

*Serial I*

Synopsis: Request captioned matter be opened and assigned to the writer.

Details: The purpose of this EC is to request captioned matter be opened and assigned to the writer. This matter is predicated based on information received from the complainant/victim organization, Government of District of Columbia (DC).

On 4/20/2012, WFO CY-4 received information that the DC's website, DC.gov, was under attack. Writer talked to [redacted] Chief Technology Officer, Office of the Chief Technology Officer (OCTO), Government of the District of Columbia, 441 4th St. NW, Washington, DC 20001, telephone number: [redacted] via telephone the same day. [redacted] reported DC.gov website was under Distributed Denial of Service (DDOS) attack since 4/18/2012 6:45pm, 25 hours into the attack, OCTO was able to restore the website and contained the DDOS attack. OCTO did not detect any intrusions into DC government's computer network. [redacted] forward writer an email contained possible perpetrators' twitter postings, postings at Pastebin.com, and a link to team-diversity.net. Within the twitter postings, user account [redacted] "UGNazi @UGNazi", [redacted] and [redacted] claimed taking down DC, New York City, and NASDAQ websites. The twitter

b6  
b7C

UNCLASSIFIED

*6/12/16.ec*

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

postings included a link to Pastebin.com posting which revealed DC city mayor Vincent C Gray's personal identification information (PII).

On 4/20/2012, writer talked to DC Metropolitan Police Department Task Force Office [REDACTED] telephone number: [REDACTED] via telephone. [REDACTED] stated the MPD was aware of the leak of DC Mayor's PII. The leaked PII was not accurate and some were outdated.

b6  
b7C

Open source search on [REDACTED] and "UGNazi @UGNazi" revealed two hacker group UGNazi, with website at UGNazi.com, and Team Diversity at team-diversity.net. UGNazi members were [REDACTED]

b6  
b7C

[REDACTED] Team Diversity members were [REDACTED]  
[REDACTED]

ACS search on [REDACTED] revealed he is the subject of New York field office's case, case number [REDACTED] UGNAZI. In serial 40, [REDACTED] identified as following:

b6  
b7C  
b7E

True Name: [REDACTED]

b6  
b7C

Alias: [REDACTED]

Monikers: [REDACTED]

Address: [REDACTED] (current)  
[REDACTED] (former)

DOB: [REDACTED]

SSN: [REDACTED]

Email: [REDACTED]  
[REDACTED]

ICQ: [REDACTED]

MSN: [REDACTED]

Skype: [REDACTED]

Twitter: [REDACTED]

Website: [REDACTED]

Based on the information above, WFO request that a Full Investigation be opened and assigned to SA [REDACTED]

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re:  04/23/2012

b7E

LEAD(s) :

Set Lead 1: (Info)

NEW YORK

AT CY2

Read and clear.

♦♦

UNCLASSIFIED

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/24/2012

On 4/24/2012, [redacted] Chief Technology Officer, Office of the Chief Technology Officer (OCTO), Government of the District of Columbia, 441 4th St. NW, Washington, DC 20001, telephone number: [redacted] email: [redacted] was interviewed in Washington, D.C. Also present during the interview were [redacted] email address: [redacted] telephone number: [redacted] cell phone number: [redacted] After being advised of the identity of the interviewing agent and the nature of the interview, [redacted] provided the following information:

b6  
b7C

[redacted] provided two CDs, one contained PCAP files and graphs from Distributed Denial of Service (DDOS) attack from 4/18/2012 to 4/19/2012, and the other contained the firewall logs from that attack. [redacted] stated the personal information on DC Mayor was not accurate and it was not the result of any computer intrusions in DC government network. DC government has not discover any other DC government employee's personal information was published on the internet.

b6  
b7C

[redacted] introduced writer to [redacted] Security Operations, Office of the Chief Technology Officer, telephone number: [redacted] email: [redacted] is the point of contact for any technical questions regarding the DDOS attack.

b6  
b7C

Gj1416.302

KCB 04/25/2012

Investigation on 4/24/2012 at Washington, DCFile # [redacted]Date dictated [redacted]by SA [redacted] :lj

b7E

b6  
b7C

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/01/2012

To: Washington Field

Attn: CY4

From: Washington Field

CY4/NVRA

Contact: [REDACTED]

Approved By: [REDACTED]

KCB 05/01/2012

Drafted By: [REDACTED]

lj

6/5/1/2012

Case ID #: [REDACTED]

Pending)

Title: UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VITIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: Documenting finding on [REDACTED]

Details: On 5/1/2012, writer found a twitter posting between [REDACTED] and [REDACTED] who is a reporter from [REDACTED]. In the posting, [REDACTED] told [REDACTED] to contact him at [REDACTED] to discuss his attacks on dc.gov website.

A Google search using on email [REDACTED] an email listed in [REDACTED]'s DOX information, revealed the following website that link the Comcast email account to the "Team Diversity" member [REDACTED]

Additional searches revealed the following information:

The third return result in Google's organic (non-paid) search returns was titled "Hack Forums - {Team Diversity} Selling GT: stfu" and located at [www.hackforums.net](http://www.hackforums.net) > Hack Forums > Marketplace > Gametags. The excerpt in the search return included the following text, "05-20-2011, 3:39 PM. GT Control Proof: Spoiler (Click to View). [Image: glQ59.jpg]. Contact AIM: XBLTime. [REDACTED]"

UNCLASSIFIED

lj12/28a.ec

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 05/01/2012

b7E

A post made to codeupload.com (codeuploade.com/4851) on 23 December 2011 at 5:15 pm UTC advertising [REDACTED] stated the following information,

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]
6. Team Diversity Gamertags
7. Team Diversity
8. Team Diversity [REDACTED]
9. <http://www.youtube.com/watch?v=bWzJZEixH9g>

b6  
b7C

The referenced YouTube post was no longer available at the time of the open source searches.

An AOL LiveStream profile using the moniker [REDACTED] contained the following, "ADD [REDACTED] on May 12 at 5:05 pm and "Selling Diversity Booter 300+ shells onlu \$10" on Jan 20 at 5:54 PM.

b6  
b7C

An Xbox Live Profile (live.xbox.com/en-US/Profile?gametag=my bolt action) lists in the BIO section the following information, "Team Diversity - [REDACTED] and "AIMs: [REDACTED] [REDACTED] YouTube.com [REDACTED].

b6  
b7C

Writer intended to subpoena registration information on these email accounts and request search warrants as well.

♦♦

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 05/01/2012

**To:** Washington Field

**Attn:** CY4

**From:** Washington Field

CY4/NVRA

**Contact:** [REDACTED]

**Approved By:** [REDACTED]

*kcb 05/01/2012*

**Drafted By:** [REDACTED]

*lj 5/1/2012*

**Case ID #:** [REDACTED] (Pending)

**Title:** UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VITIM;  
COMPUTER INTRUSION - CRIMINAL

**Synopsis:** Documenting email communication with New York office.

**Details:** On 4/27/2012, writer received a email from SSA [REDACTED]  
[REDACTED] regarding terminating the lead to Los Angeles to interview  
possible suspect [REDACTED] in order to avoid operational conflict  
with the FBI New York investigation. Writer will continue all  
other logical investigative steps to move case forward.

♦♦

UNCLASSIFIED

*- lj 12/28/12.ec*

b6  
b7C

b7E

b6  
b7C

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 04/23/2012

**To:** Washington Field  
New York  
Minneapolis  
  
Phoenix

**Attn:** SA [redacted]  
**Attn:** SSA [redacted]  
**Attn:** SSA [redacted]  
SA [redacted]  
**Attn:** SSA [redacted]

b6  
b7C

**From:** Washington Field  
ID-3, CY-4/NVRA/3E  
**Contact:** IA [redacted]

b6  
b7C

**Approved By:** [redacted]

*MJD 5/3/12*  
*BAS 10/7/2012*

**Drafted By:** [redacted]

itab

*STAB 4/24/2012*

**Case ID #:** [redacted]

174C-MP-74385 (Pending) - 15

b7E

**Title:** UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

UNSUB(s):

AKA [redacted]  
AKA [redacted]  
AKA [redacted]

CHASKA POLICE DEPARTMENT, (VICTIM)  
02/22/2012,  
TELEPHONE BOMB THREATS

b6  
b7C

**Synopsis:** (U) To document open source searches revealing DDoS, hacking and doxing activity by members of the UGNazi Hacktivist Group.

**Enclosure(s):** Print-outs of referenced web pages will be maintained to the captioned investigation's case file via 1A.

**Details:** (U//~~FOUO~~) By way of background, Washington Field Office (WFO) squad CY-4 opened the captioned investigation into the hacktivist group "UGNAZI" in April 2012 based on the group's claims of responsibility for online attacks targeting computer network infrastructure belonging to the District of Columbia

12ja114b.ec

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

(Reference [REDACTED] for details). Open source searches for UGNAZI and the following identified group members

b7E

[REDACTED]  
revealed the following information.

b6  
b7C

(U) A 19 April 2012 post to the "UGNaziNews" (twitter.com/#!/UGNaziNews) Twitter feed, hereafter referred to as UGNaziNews Twitter, by [REDACTED]

[REDACTED] hereafter referred to as [REDACTED] stated, [REDACTED]

b6  
b7C

[REDACTED] The hyperlinked text ending in [REDACTED] linked to an image at the Uniform Resource Locator (URL) [REDACTED] that displayed a web page not available error message for nyc.gov. The hyperlinked text ending in [REDACTED] linked to an image at the URL [REDACTED] that displayed a web page not available error for dc.gov.

(U) A 19 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]

b6  
b7C

[REDACTED] The hyperlinked URL linked to a news story about the Hacker Group UGNazi conducting Distributed Denial of Service (DDoS) attacks against dc.gov and nyc.gov as an act of protest against the US Government.

(U) A 19 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]

b6  
b7C

[REDACTED] The hyperlinked text ending in [REDACTED] linked to an image at the URL [REDACTED] that displayed a web page not available error for washington.org.

(U) A 19 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]

b6  
b7C

[REDACTED] The hyperlinked pastebin URL linked to a pastebin post that contained Personal Identifying Information (PII) for Washington DC Mayor Vincent Gray; including Date of Birth (DOB), Social Security Number (SSN), phone numbers and addresses.

(U) A 19 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]

b6  
b7C

[REDACTED] The hyperlinked

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

URL linked to an image at [REDACTED] that displayed a web page not available error for nasdaq.com.

b6  
b7C

(U) A 20 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]. The hyperlinked URL linked to an image at [REDACTED] that displayed a web page not available error for [REDACTED]

b6  
b7C

(U) A 20 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]. The hyperlinked URL linked to an image at [REDACTED] that displayed a web page not available error for wa.gov.

b6  
b7C

(U) A 23 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED]. The hyperlinked pastebin URL linked to pastebin post that contained a message apparently protesting the Cyber Intelligence Sharing and Protection Act - H.R. 3523 and listing the following pastebin URLs under the claim, [REDACTED]

b6  
b7C

The post goes on to claim to release a U.S. District court order for [REDACTED] at the URL [REDACTED]

(U) The hyperlinked URL [REDACTED] linked to a pastebin post made in apparent retaliation for law enforcement actions against LulzSec members [REDACTED]

b6  
b7C

and in protest of [REDACTED] UGNazi member [REDACTED] claimed to have [REDACTED] and listed alleged FBI.gov server details, FBI Intranet vulnerabilities, and d0xed 7 FBI agents allegedly involved in brining down LulzSec. The 7 alleged FBI agents d0xed in the post were: [REDACTED]

[REDACTED] The d0x listed credit card numbers, CVC2s, fbi.gov email addresses and passwords. The email [REDACTED]

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

addresses did not conform to the format used by FBI email accounts used on either unclassified or classified networks.

(U) FBI intranet directory searches on the names of aforementioned d0xed agents did not return BPMS directory listings for FBI employees; with the exception of [REDACTED] which returned information on a [REDACTED] whose work telephone number indicated he works out of [REDACTED]

b6  
b7C

(U) The hyperlinked [REDACTED] linked to a pastebin post that listed PII for 5 alleged "CIA Field Agents". The post claimed the PII was obtained by hacking cia.gov email accounts.

b6  
b7C

(U) A 23 April post to the UGNaziNews Twitter feed by the [REDACTED] the [REDACTED] Twitter profile [REDACTED], hereafter referred to as [REDACTED] Twitter, stated, "#FBI Document leaked - [REDACTED] The hyperlinked pastebin URL linked to the aforementioned pastebin post tweeted by [REDACTED]

b6  
b7C

(U) A 23 April 2012 post to the UGNaziNews Twitter feed by [REDACTED] stated, [REDACTED] [REDACTED]. The hyperlinked URL linked to an image at [REDACTED] that displayed a web not available error for cia.gov.

b6  
b7C

(U) A 23 April post to the UGNaziNews Twitter feed by the owner/operator of the UGNazi Twitter profile [REDACTED] hereafter referred to as the UGNazi Twitter, stated, [REDACTED]

b6  
b7C

(U) A 23 April 2012 post to the UGNazi Twitter feed by the [REDACTED] the Twitter account [REDACTED] [REDACTED], hereafter referred to as [REDACTED] stated, [REDACTED]

b6  
b7C

By [REDACTED] The hyperlinked [REDACTED] URL linked to a [REDACTED] post that contained a 19 page (when printed) list of PII for [REDACTED] and his family, as well as what appeared to be content of email messages in which [REDACTED] indicates that he "swatted" people.

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

(U) The [REDACTED] d0x contained a URL to an image at [REDACTED] which displayed what appeared to be the contact page for an online bank account or credit card account manager for an account belonging to [REDACTED]. Based on the location of the URL in the d0x, right below [REDACTED]'s Visa credit card information, it is assessed with medium confidence that this screen shot image may be for an account manager page tied to that credit card.

b6  
b7C

(U//~~FOUO~~) An ACS search revealed a connection between [REDACTED] and a series of telephonic bomb threats being investigated by FBI Minneapolis Division (See [REDACTED] for details).

b6  
b7C  
b7E

(U//~~FOUO~~) The following emails listed in the [REDACTED] d0x were run as search terms in ACS. The search yielded one positive result for the email [REDACTED]. The serial documented open source derived information which tied the email account to the name [REDACTED] which is very similar to the alias [REDACTED] listed in the UGNazi d0x of [REDACTED] (See 174C-MP-74385, serial 9 for details). The d0x also lists [REDACTED] as [REDACTED]'s AOL Instant Messenger ID which is consistent with references to [REDACTED] documented to [REDACTED].

b6  
b7C

b7E

(U//~~FOUO~~) [REDACTED]

b6  
b7C  
b7E

(U) The [REDACTED] d0x is further corroborated by a YouTube profile for [REDACTED] that contained the following comments dealing with swatting:

b6  
b7C

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

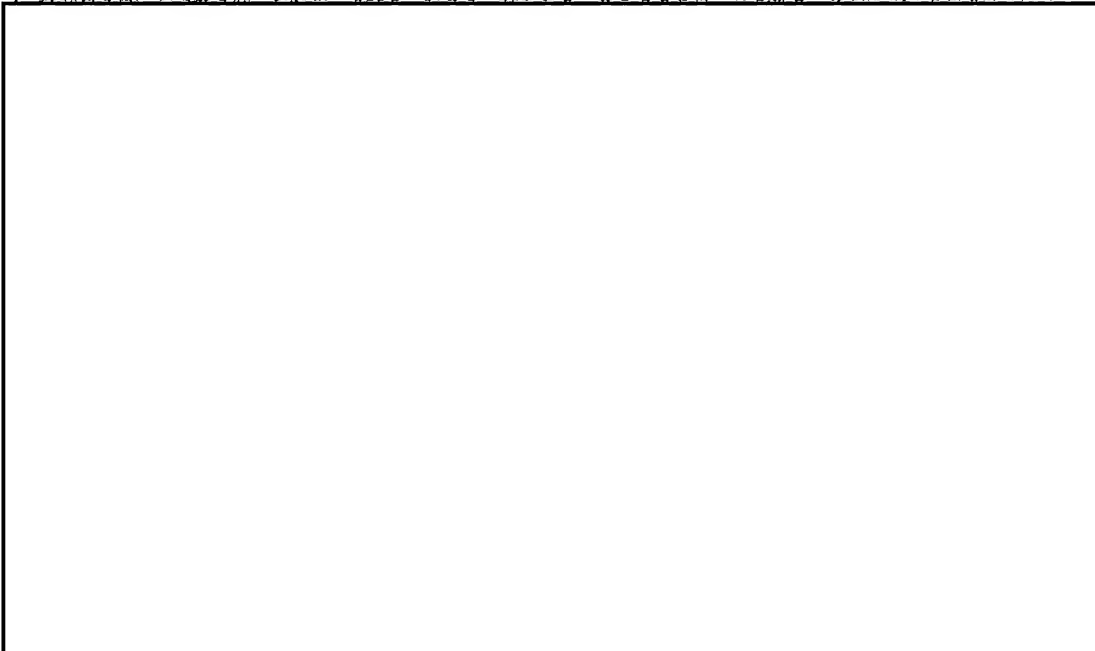
b7E



b6  
b7C

**Analysis:**

(U//~~FOUO~~) It is assessed with high confidence that the UGNazi hacktivist group did not compromise FBI or CIA employee email accounts as claimed in the aforementioned d0xing posts and NYO ADIC letter post made by UGNazi members to pastebin. This assessment is based on the following indicators that suggest the FBI d0xing information and the NYO ADIC letter were fabrications.



b6  
b7C  
b7E

(U//~~FOUO~~) It is assessed with medium to high confidence that the d0x published by the UGNazi hacktivist group targeting [REDACTED] [REDACTED] is true information possibly obtained by UGNazi members through the compromise of one or more of the email accounts listed in the d0x. This assessment is based upon the preponderance of corroborating information listed below.

b6  
b7C

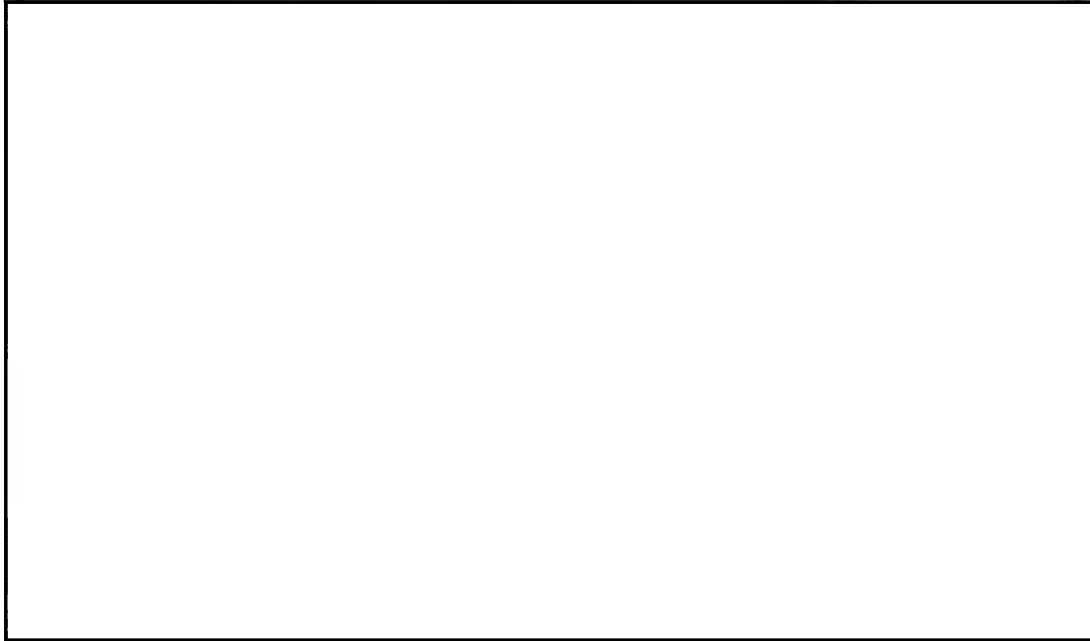


b6  
b7C  
b7E

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E



b6  
b7C  
b7E

(U//~~FOUO~~) Based on the aforementioned details corroborating the [REDACTED] d0x it is assessed with medium confidence that one or more members of the UGNazi hacktivist group are capable (both in motivation and skill level) of committing computer network intrusion and/or social engineering resulting in the compromise of online password protected accounts.

b6  
b7C

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

**Accomplishment Information:**

Number: 1

Type: SUBJECT IDENTIFIED

ITU: [REDACTED]

Claimed By:

SSN:

Name:

Squad:

[REDACTED]

b6  
b7C  
b7E

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

To: Washington Field From: Washington Field  
Re: [REDACTED] 04/23/2012

b7E

LEAD(s) :

Set Lead 1: (Info)

NEW YORK

AT NEW YORK, NY

For New York Field Office Squad CY-2's situational awareness. Read and clear.

Set Lead 2: (Info)

MINNEAPOLIS

AT MINNEAPOLIS, MN

For Minneapolis Field Office Squad CT-3's situational awareness. See the information regarding the possible true identity of [REDACTED] and alleged evidence of swatting activity documented on pages 4 - 6 of the enclosed communication. The full text of the [REDACTED] report are enclosed in the accompanying 1A. Read and clear.

b6  
b7C  
b7E

Set Lead 3: (Info)

PHOENIX

AT PHOENIX, AZ

For Phoenix Field Office Squad C-2's situational awareness regarding d0xing victims and possible case subject residing in Phoenix's AOR. Read and clear.

♦♦



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/11/2012

To: Cyber

Attn: SSA [redacted]  
SSA [redacted]

b6  
b7C

To: Charlotte

Attn: SSA [redacted]

To: Dallas

Attn: SSA [redacted]

To: Houston

Attn: SSA [redacted]

To: Los Angeles

Attn: Cyber SSA CY-1

To: Little Rock

Attn: SSA [redacted]

To: New York

Attn: SSA [redacted]

From: Washington Field

CY-4/NVRA/Room 3E-128

Contact: [redacted]

b6  
b7C

Approved By: [redacted]

*KCB 05/11/2012*

Drafted By: [redacted]

kcb

Case ID #: [redacted]

b7E

Title: UGNAZI;  
TEAM DIVERSITY;  
DC.GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: To document notification and liaison contact made with  
Special Agent (SA) [redacted]  
Office of Inspector General (OIG) on 05/11/2012.

b6  
b7C

Attachment: E-mail communication from Supervisory Special Agent (SSA) [redacted]  
[redacted] regarding a distributed denial of service attack (DDoS) of  
the [redacted] web site dated 05/11/2012.

b6  
b7C  
b7E

Details: On 05/11/2012, SSA [redacted] contacted SSA [redacted] via UNET e-  
mail advising of a DDoS attack of the [redacted] web  
page apparently conducted by members of "UGNazi", including  
individuals utilizing the monikers [redacted] respectively.

b6  
b7C  
b7E

On this same date, via e-mail and telephone conversations,  
SSA [redacted] advised [redacted] liaison contacts of this

b6  
b7C

UNCLASSIFIED

131kbec1.wpd

UNCLASSIFIED

To: Cyber From: Washington Field  
Re: [REDACTED] 05/11/2012

b7E

possible DDoS. SA [REDACTED] later confirmed their web site had in fact been DDoSed but was now currently up and running. SA [REDACTED] is

b6  
b7C  
b7E  
b5

[REDACTED]  
the District of Columbia United States Attorney's Office for a prosecutive opinion. SA [REDACTED] advised he may [REDACTED]

[REDACTED] once he has a better understanding of the incident.

SA [REDACTED] advised the [REDACTED] had network infrastructure at three locations including [REDACTED]  
[REDACTED] SA [REDACTED] further advised through open source research he identified Twitter feeds of individuals claiming responsibility for the DDoS of his organization. WE will continue coordination efforts with the [REDACTED] on this matter.

b6  
b7C  
b7E

On 05/11/2012, SSA [REDACTED] forwarded a copy of the attached e-mail thread related to this incident to all identified field offices with potential equities in this matter for their situational awareness.

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Washington Field  
Re:  05/11/2012

b7E

Set Lead 1: (Info)

CYBER

AT WASHINGTON, DC

For information.

Set Lead 2: (Info)

CHARLOTTE

AT CHARLOTTE, NC

For information.

Set Lead 3: (Info)

DALLAS

AT DALLAS, TX

For information.

Set Lead 4: (Info)

HOUSTON

AT HOUSTON, TX

For information.

UNCLASSIFIED

UNCLASSIFIED

To: Cyber From: Washington Field  
Re: [REDACTED] 05/11/2012

b7E

Set Lead 5: (Info)

LOS ANGELES

AT LOS ANGELES, CA

For information.

Set Lead 6: (Info)

LITTLE ROCK

AT LITTLE ROCK, AR

For information.

Set Lead 7: (Info)

NEW YORK

AT NEW YORK, NY

For information.

♦♦

UNCLASSIFIED

[redacted]  
From: [redacted]  
Sent: Friday, May 11, 2012 10:45 AM  
To: [redacted]  
Cc: [redacted]  
Subject: FW: [redacted]

b6  
b7C  
b7E

See the below re a confirmed DDoS of the [redacted] website purportedly conducted by members of UGNazi to include [redacted] My [redacted] OIG POC advised they had infrastructure in three places including [redacted] He is checking to determine the other locations and which were effected and will get back to me.

[redacted]  
SSA [redacted]  
FBI/WFO/NVRA/CY-4  
[redacted] (D)  
[redacted] (C)  
703.686.6010 (F)

b6  
b7C  
b7E

-----Original Message-----

From: [redacted]  
Sent: Friday, May 11, 2012 9:49 AM  
To: [redacted]  
Subject: RE: [redacted]

b6  
b7C  
b7E

[redacted]  
[redacted] once they get a better handle on the incident. Once they get back to me I will update you.

b7E  
b5

[redacted]  
SSA [redacted]  
FBI/WFO/NVRA/CY-4  
[redacted] (D)  
[redacted] (C)  
703.686.6010 (F)

b6  
b7C

-----Original Message-----

From: [redacted]  
Sent: Friday, May 11, 2012 8:09 AM  
To: [redacted]  
Cc: [redacted]  
Subject: Re: [redacted]

b6  
b7C  
b7E

b6  
b7C

KCB  
05/11/2012

b7E

I am a Cyber Squad Supervisor in the WF Office and the [redacted] is in my AOR. I appreciate any information you have on the subjects involved in the [redacted]

b7E

I can be reached @ [redacted] and BB [redacted] Thanks in advance for your assistance.

b6  
b7C

----- Original Message -----

From: [redacted]

To: [redacted]

Cc: [redacted]

Sent: Fri May 11 07:51:38 2012

Subject: Re: [redacted]

b6  
b7C  
b7E

[redacted]  
Please see below in regards to a DDoS attack attributed to [redacted]

b6  
b7C

----- Original Message -----

From: [redacted]

To: [redacted]

Cc: [redacted]

Sent: Thu May 10 23:12:11 2012

Subject: [redacted]

b6  
b7C  
b7E

b6  
b7C

[redacted]  
[redacted] is currently down due to DDoS attack by [redacted] and members of UGNazi to include [redacted] I believe I have PII for [redacted] to include name and home address. Can you provide contact info for the agent looking into [redacted]? My notes from today's meeting are at the office and I will be out until May 21.

b6  
b7C  
b7E

Twitter accounts for individuals captioned above are:

[redacted]

b6  
b7C

I'll keep you updated as info comes in.

[redacted]

b6  
b7C

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/07/2012

To: Washington Field

Attn: CY-4

From: Washington Field

CY4/NVRA

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(Pending)

Title: UGNAZI - UGNAZI;  
TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: Requesting a STATS sub file to be opened.

Details: Writer requesting a STATS sub file to be opened under captioned case in order to record all the statistical accomplishments.

♦♦

O&A(Main/Sub) SMS  
Closed: 64 / C5 / C6  
Class & Alpha -WF-  
Source 1  
CPI Codes (1) CRINT-C  
(2) MIP200  
PI     / Full      
Begins     /     /     Expires     /     /      
Assign To     /     /    

*SH 5/9/2012*

UNCLASSIFIED

*lj 12135c.ec*

b6  
b7C

b7E

b6  
b7C





U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to

File No. [REDACTED]

Northern Virginia Resident Agency  
9325 Discovery Blvd.  
Manassas, VA 20109

b7E

May 2, 2012

Long Beach Police Department  
Computer Crimes Detail

RE: Distributed Denial of Service (DDOS) attack on DC.gov website  
from 4/18/2012 to 4/19/2012.

Dear Detective [REDACTED]

b6  
b7C

On 4/20/2012, the FBI Washington Field Office received information that the DC's website, DC.gov, was under DDOS attack. FBI Special Agent (SA) [REDACTED] talked to [REDACTED] Chief Technology Officer, Office of the Chief Technology Officer (OCTO), Government of the District of Columbia, 441 4th St. NW, Washington, DC 20001, telephone number: [REDACTED] via telephone the same day. [REDACTED] reported DC.gov website was under Distributed Denial of Service (DDOS) attack since 4/18/2012 6:45pm, 25 hours into the attack, OCTO was able to restore the website and contained the DDOS attack. OCTO did not detect any intrusions into DC government's computer network. [REDACTED] sent SA [REDACTED] an email in which contained postings on twitter.com, Pastebin.com, and a link to team-diversity.net. Within the twitter postings, user account [REDACTED]

b6  
b7C

[REDACTED] claimed taking down DC government, New York City, and NASDAQ websites. In a twitter posting between [REDACTED] who is a reporter from dcist.com, [REDACTED] told [REDACTED] to contact him at [REDACTED] to discuss the DDOS attacks on dc.gov website. Further search in twitter postings revealed a link to Pastebin.com posting which posted DC city mayor Vincent C Gray's personal identification information (PII).

On 4/20/2012, writer talked to DC Metropolitan Police Department Task Force Office [REDACTED] telephone number: [REDACTED] via telephone. [REDACTED] stated the MPD was aware of the leak of DC Mayor's PII. The leaked PII was not accurate and some information were outdated.

b6  
b7C

Internet search on [REDACTED] revealed two hacker group UGNazi, with website at UGNazi.com, and Team Diversity at team-diversity.net. UGNazi.com listed its members as [REDACTED]

b6  
b7C

[redacted] Team-Diversity.net listed its members as  
[redacted]

b6  
b7C

Following items are attached to this Letter: a CD contained screen shots of twitter postings and online articles regarding DDOS attack on DC.gov, a CD contained PCAP file, and a CD contained firewall log on DDOS attack.

The above information is provided to you for action as deemed appropriate. Questions regarding this matter can be directed to SA [redacted] Squad CY-4 (located at the Northern Virginia Resident Agency), [redacted]

b6  
b7C

Sincerely,

Ronald T Hosko  
Special Agent in Charge

By: [redacted]  
[redacted]

Supervisory Special Agent

b6  
b7C

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/15/2012

To: Washington Field

Attn: CY4

From: Washington Field

CY4/NVRA

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #:

[REDACTED] (Pending)

Title: UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VITIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: Documenting finding on [REDACTED]

Details: On 5/2/2012, FBI Task Force Officer (TFO), Long Beach Police Department Sgt. [REDACTED] contacted writer via email and provided following information:

[REDACTED] was arrested for numerous computer related crimes by the Long Beach Police Department (LBPd) and is due in court later in May 2012. He has been positively identified and search warrants have been served. Some of his computers are in LBPd custody. The handling LBPd Detective is [REDACTED] telephone number: [REDACTED] [REDACTED] has done lots of work on [REDACTED] and his friends. [REDACTED]s personal information are following:

DOB: [REDACTED]

Cell phone: [REDACTED]

Address: [REDACTED]

Subjects Mother:

Address: [REDACTED]

Employer: [REDACTED]

Work Phone: [REDACTED]

Cell: [REDACTED]

UNCLASSIFIED

Gj13812.ec

b6  
b7C

b7E

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 05/15/2012

b7E

On 5/3/2012, TFO [REDACTED] contacted writer via email and provided a list of the subjects who were identified by Detective [REDACTED]. The following list was compiled from the SWATTING and ID theft case Detective [REDACTED] is investigating:

b6  
b7C

AKA: [REDACTED]  
Name: [REDACTED]  
DOB: [REDACTED]  
M/W [REDACTED]  
Address: [REDACTED]  
Home: [REDACTED]  
Mom: [REDACTED]  
Cell: [REDACTED]  
AIM: [REDACTED]  
Twitter: [REDACTED]  
Facebook: [REDACTED]  
YouTube: [REDACTED] (videos show DDoS of TacoBell.com and theft of Xbox game tags.)  
Web page: [REDACTED] (Possibly contains virus) Site shows members are [REDACTED]  
Groups: [REDACTED]  
Notes: I have several PayPal transactions regarding the purchase of VPN accounts. Search warrant served on residence in November 2011 and computers taken. [REDACTED]

b6  
b7C

[REDACTED]

AKA: [REDACTED]  
Name: [REDACTED]  
DOB: [REDACTED]  
M/W [REDACTED]  
Address: [REDACTED]  
AIM: [REDACTED]  
Notes: [REDACTED]

[REDACTED]

[REDACTED] Due to the subject being [REDACTED] years old at the time, no case was filed. [REDACTED]

b6  
b7C  
b7E

AKA: [REDACTED]  
Name: [REDACTED]  
DOB: [REDACTED]  
M/W [REDACTED]

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 05/15/2012

b7E

Address: [REDACTED]

Home: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C  
b7E

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

CDL: [REDACTED]

Cell: [REDACTED]

M/W: [REDACTED]

Address: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

Address: [REDACTED]

Home: [REDACTED]

Cell: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

Address: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

Lives with: [REDACTED]

Address: [REDACTED]

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 05/15/2012

b7E

Home: [REDACTED]

AIM: [REDACTED]

ISP: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

M/W [REDACTED]

Address: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

M/W [REDACTED]

Address: [REDACTED]

Home: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

AKA: [REDACTED]

name: [REDACTED]

DOB: [REDACTED]

M/W [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

AKA: [REDACTED]

Name: [REDACTED]

DOB: [REDACTED]

Male [REDACTED]

Address: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED], 05/15/2012

b7E

On 5/4/2012, writer received a email from SA [REDACTED]  
[REDACTED] Los Angeles Division. A copy of LBPD report on [REDACTED] was  
attached to the email. The LBPD report was prepared by Detective  
[REDACTED] and it detailed the investigation conducted for  
[REDACTED]

b6  
b7C

♦♦

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 05/15/2012

**To:** Baltimore

**Attn:** Cyber Squad

**From:** Washington Field

CY4/NVRA

**Contact:** [REDACTED]

**Approved By:** [REDACTED]

CB 05/17/2012.

**Drafted By:** [REDACTED]

lj

5/15/2012

**Case ID #** [REDACTED]

(Pending)

**Title:** UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

**Synopsis:** Request concurrence from Baltimore Field Office to conduct interview in Annapolis, MD.

**Details:** On 4/20/2012, Washington Field Office (WFO) CY-4 received information that the DC's website, DC.gov, was under Distributed Denial of Service (DDoS) attack. During the course of the investigation, writer determined the members of hacker group UGNazi and Team Diversity were behind attack. Group member

[REDACTED] DOB: [REDACTED] address: [REDACTED]  
[REDACTED] were positively identified by Long Beach Police Department (LBPd) during their investigation. LBPd provided WFO with information on [REDACTED] as well as several [REDACTED]

[REDACTED] The following individual resides in [REDACTED]

**AKA:** [REDACTED]

**Name** [REDACTED]

**DOB:** [REDACTED]

**M/W** [REDACTED]

**Address:** [REDACTED]

**Home:** [REDACTED]

**AIM:** [REDACTED]

**Notes:** [REDACTED]

UNCLASSIFIED

md\_interview\_req.wpd



UNCLASSIFIED

To: Baltimore From: Washington Field  
Re: [REDACTED] 05/15/2012

b7E

Writer intends to interview [REDACTED] to determine his involvement in the DDoS attack against DC.gov and any other illegal online activities.

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Baltimore From: Washington Field  
Re: [REDACTED] 05/15/2012

b7E

Set Lead 1: (Info)

BALTIMORE

AT CYBER SQUAD

Requesting concurrence to travel to  
Annapolis, MD to interview [REDACTED]  
♦♦

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 05/18/2012

**To:** Washington Field

**Attn:** SA [REDACTED]  
CY-04

b6  
b7C

**From:** New York  
CY-02

**Contact:** SA [REDACTED]

**Approved By:** [REDACTED]

**Drafted By:** [REDACTED] *file*

**Case ID #:** [REDACTED]

b7E

**Title:** OPERATION CARDSHOP

UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VITIM;  
COMPUTER INTRUSION - CRIMINAL

**Synopsis:** To request Washington Field to delay contact with individuals associated with UG Nazi.

**Administrative:** The following was emailed on May 17, 2012 as a follow up to a phone conversation.

**From:** [REDACTED]  
**Sent:** Thursday, May 17, 2012 2:29 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]

b6  
b7C

**Subject:** RE: interviews

Good afternoon [REDACTED]

b6  
b7C

I appreciate the heads up regarding the information below. As per our phone conversation, please wait until the coordinated takedown, scheduled for June 26, 2012, to contact these guys.

We are unfamiliar with [REDACTED] at the moment, but [REDACTED] is a registered member of our UC forum. Many of the UG guys have

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: New York  
Re: [REDACTED] 05/18/2012

b7E

direct connection with our UC forum and it will not be advisable to approach them prior to June 26.

Lastly, [REDACTED] is out of the office and will be back on Monday. He'll work on getting those logs to you next week.

b6  
b7C

Thanks!

[REDACTED]

b6  
b7C

From: [REDACTED]  
Sent: Thursday, May 17, 2012 8:42 AM  
To: [REDACTED]  
Cc: [REDACTED]  
Subject: interviews

b6  
b7C

Hey guys, I got a list of names from long beach pd det [REDACTED] Those are the ppl Det [REDACTED] identified in his investigation into [REDACTED] and they associated with [REDACTED] online. I notice there are couple of guys live close by to dc, would like to interview them regarding their role in DC.gov attack and any other illegal activities. Just want to be a team player and make sure not stepping over each other. Oh by the way, [REDACTED] did you get chance to sent out those logs from NY.gov and NASDAQ.com attacks? thanks

b6  
b7C

AKA: [REDACTED]

Name [REDACTED]

DOB: [REDACTED]

M/W [REDACTED]

Address: [REDACTED]

Home: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

b6  
b7C

AKA: [REDACTED]

Name [REDACTED]

DOB: [REDACTED]

M/W [REDACTED]

Address: [REDACTED]

Home: [REDACTED]

AIM: [REDACTED]

Notes: [REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: New York  
Re: [REDACTED] 05/18/2012

b7E

[REDACTED]

b6  
b7C

**Details:** New York respectfully requests Washington Field to delay contact with the individuals associated with UGNazi, to include the members mentioned above.

b7E

[REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: New York  
Re:  05/18/2012

b7E

LEAD(s) :

Set Lead 1: (Info)

WASHINGTON FIELD

AT WASHINGTON, DC

New York respectfully requests Washington Field to delay contact with the individuals associated with UGNazi, to include the members mentioned above.

♦♦

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/22/2012

To: Washington Field

Attn: CY-4

From: Washington Field

CY4/NVRA

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(Pending)  
(Pending)

Title: UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: Reporting investigation conducted.

Details: From 5/2/2012 to 5/18/2012, through twitter postings by [REDACTED] at [REDACTED] and third party reporting, writer learned hacker group UGNazi was involved in attacks on IC3.gov, ed.gov, Washington Military Department website, ca.gov, Government of Anguilla (gov.ia), visa.com, cia.gov, wtf.com, Discover.com.

Pertaining to attack on wtf.com, information indicated UGNazi hacked its registration information. Writer did a Domaintools lookup on wtf.com and find following as the registration information:

Registrant:  
UGNazi, Inc.  
ATTN WTF.COM  
care of Network Solutions  
PO Box 459  
Drums, PA. US 18222  
Administrative Contact, Technical Contact: [REDACTED]

Created: 1995-08-12  
Expires: 2019-08-11  
Updated: 2012-05-17

UNCLASSIFIED

Lj14572.ec

b6  
b7C

b7E

b6  
b7C

b6  
b7C

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 05/22/2012

b7E

Writer contacted [REDACTED] Investigator at  
Network Solutions, telephone number: [REDACTED]  
[REDACTED] fax number: 703-668-5959,  
via telephone on 5/22/2012. [REDACTED] confirmed that wtf.com is  
registered through Network Solutions; the real registrant  
information and domain management account login information are  
available upon request through a subpoena.

b6  
b7C

♦♦

UNCLASSIFIED



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

Precedence: ROUTINE

Date: 05/24/2012

To: Washington Field

Attn: CY-4

From: Washington Field

CY4/NVRA

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #:

[REDACTED] Pending)  
[REDACTED] (Pending)

Title: UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

Synopsis: Reporting AUSA's response.

Details: On 5/17/2012, writer submitted a subpoena request for registrant information on wtf.com to Assistant US Attorney [REDACTED] for approval. On 5/24/2012, [REDACTED] contact writer via telephone to advised prosecutor in Washington DC [REDACTED]

[REDACTED] Writer will forward all the information on wtf.com intrusion to Detective [REDACTED] telephone: [REDACTED], email: [REDACTED] Long Beach Police Department for his case.

♦♦

UNCLASSIFIED

lj 15312.ec

b6  
b7C

b7E

b6  
b7C  
b5

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/08/2012

From 5/2/2012 to 5/18/2012, through twitter postings by [ ] at [ ] and third party reporting, writer learned hacker group UGNazi was involved in attacks on IC3.gov, ed.gov, Washington Military Department website, ca.gov, Government of Anguilla (gov.ia), visa.com, cia.gov, wtf.com, Discover.com.

b6  
b7C

Pertaining to attack on wtf.com, writer conducted another domain lookup on wtf.com on 5/24/2012 and find following as the registration information:

## Registrant:

Wtf, Inc.  
4550 Ocala Drive  
Parma, OH 44134  
US

Administrative Contact, Technical Contact:

[ ]

b6  
b7C  
b6  
b7C

On 4/24/2012, [ ] telephone number: [ ] email: [ ] was interviewed via telephone. After being advised of the identity of the interviewing agent and the nature of the interview, [ ] provided the following information:

[ ] noticed his website wtf.com was redirected to ugnazi.com on 5/16/2012 and at same time he could not access his domain management account at Network Solution and his emails with Cox.net and Google. [ ] has phone and internet services through Cox.net, when he contacted Cox, he found out his account was compromised, and call forwarding was setup so all his call were forwarded to [ ] at [ ] [ ] tried to call himself, but instead of going to his voice mail like it used to, he reported someone picked up the call and did not say anything. [ ] also recalled a backup email for his Cox account was changed to an email beginning with [ ] ending in ".com". [ ] stated his domain management account at Network Solution was compromised and wtf.com registrant information was changed on 5/17/2012 around 12:30 am. [ ] talked with [ ] LNU at Network Solution, 570-708-8700, ext [ ] Network Solution generated a service ticket for this incident, ticket number [ ] Additionally, two technical contacts were

b6  
b7CInvestigation on 6/5/2012 at Washington DC (via facsimile)

File # [ ] Date dictated [ ]

by SA [ ]

b7E

b6  
b7C

6/16/12, 302

b7E

Continuation of FD-302 of [REDACTED]

. On 6/5/2012

, Page 2

b6

b7C

created, as far as [REDACTED] could recall, one was [REDACTED] and the other was [REDACTED] at UGNazi.com Inc. [REDACTED] stated he has no relationship with any members of UGNazi and doesn't know why he was targeted. All of his accounts have since been reinstated.

b6

b7C

[REDACTED] is willing to provide the login logs for his Gmail and Network Solutions accounts.

b6

b7C

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 06/12/2012

**To:** Washington Field

**Attn:** CY-4

**From:** Washington Field

CY4/NVRA

**Contact:** [REDACTED]

**Approved By:** [REDACTED]

26/12 MR/KCB

**Drafted By:** [REDACTED]

lj

6/12/2012

**Case ID #:** [REDACTED]

(Pending)

**Title:** UGNAZI - UGNAZI; TEAM-DIVERSITY;  
DC GOV - VICTIM;  
COMPUTER INTRUSION - CRIMINAL

**Synopsis:** Reporting investigation conducted.

**Details:** On 6/7/2012, writer received an email with spreadsheet attachment named "Login History.xls" from [REDACTED] Investigator at Network Solutions (NS), [REDACTED]

The spreadsheet contained login information for domain management account for wtf.com. NS released this information to the FBI upon receiving a written consent from the owner of the wtf.com, [REDACTED]. The following is the login history:

**Login History for Account #** [REDACTED]

Date	Success	Person-Org ID	IP Address	Relationship
5/17/2012 17:12	FALSE	[REDACTED]	[REDACTED]	Primary
5/17/2012 17:10	FALSE			Primary
5/17/2012 17:09	FALSE			Primary
5/17/2012 15:33	FALSE			Primary
5/17/2012 15:31	FALSE			Primary
5/17/2012 15:30	FALSE			Primary
5/17/2012 15:30	FALSE			Primary
5/17/2012 15:29	FALSE			Primary
5/17/2012 2:00	TRUE			Primary
5/17/2012 2:00	FALSE			Primary
5/17/2012 1:48	TRUE			Primary

UNCLASSIFIED

lj 17012.ec

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 06/12/2012

b7E

5/17/2012 0:17	TRUE	[REDACTED]	Primary
5/17/2012 0:07	TRUE	[REDACTED]	Primary
5/17/2012 0:07	FALSE	[REDACTED]	Primary
5/17/2012 0:06	TRUE	[REDACTED]	Primary
5/17/2012 0:04	TRUE	[REDACTED]	Primary
5/16/2012 23:59	TRUE	[REDACTED]	Primary
5/16/2012 21:53	TRUE	[REDACTED]	Primary
5/16/2012 21:14	TRUE	[REDACTED]	Primary
5/16/2012 21:13	FALSE	[REDACTED]	Primary
5/16/2012 21:04	TRUE	[REDACTED]	Primary
5/16/2012 20:55	TRUE	[REDACTED]	Primary
5/16/2012 20:45	TRUE	[REDACTED]	Tech
5/16/2012 20:44	TRUE	[REDACTED]	Primary
5/16/2012 20:40	TRUE	[REDACTED]	Primary
5/16/2012 19:37	TRUE	[REDACTED]	Primary
5/16/2012 19:09	TRUE	[REDACTED]	Primary
5/16/2012 15:32	TRUE	[REDACTED]	Tech
5/16/2012 12:32	TRUE	[REDACTED]	Tech
5/16/2012 12:32	FALSE	[REDACTED]	Tech
5/16/2012 1:51	TRUE	[REDACTED]	Tech
5/16/2012 0:23	TRUE	[REDACTED]	Tech
5/16/2012 0:19	TRUE	[REDACTED]	Tech
5/16/2012 0:19	TRUE	[REDACTED]	Tech
2/10/2012 17:24	TRUE	[REDACTED]	Primary
2/10/2012 17:19	FALSE	[REDACTED]	Primary
2/10/2012 17:19	FALSE	[REDACTED]	Primary

b6  
b7C

[REDACTED] reported [REDACTED] is his home IP address.

IP address [REDACTED] resolved to [REDACTED]  
Domain name: [REDACTED]  
Registrar: [REDACTED]  
Whois Server: [REDACTED]  
Registrant Contact: [REDACTED]  
[REDACTED]  
[REDACTED]

b6  
b7C

Fax: [REDACTED]  
[REDACTED]

IP addresses [REDACTED] resolved to [REDACTED]  
[REDACTED]

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

To: Washington Field From: Washington Field  
Re: [REDACTED] 06/12/2012

b7E

[REDACTED]

b6  
b7C

IP address [REDACTED] resolved to

[REDACTED]

There are three Person-Org ID associate with all the  
logins, [REDACTED] NS indicated these are the  
user account IDs; each contained user personal information.  
Information on these user accounts are pending from NS.

♦♦

UNCLASSIFIED